



Fair Opportunity Notice of Intent

Quality and Independent Verification and Validation (IV&V) Services for Delivery

Solicitation No. 70SBUR21R00000024

Section A—Cover Page

To: CIO-SP3 Small Business Contractors – Track 2: CIO Support

From: Anthony Pellegrino, Contracting Officer

Subject: CIO-SP3 Small Business – Fair Opportunity Notice of Intent

All holders of a contract under the multiple award Indefinite Delivery Indefinite Quantity (IDIQ) identified in the “To:” line above are invited to submit offers for consideration by the USCIS Office of Contracting in accordance with *FAR 16.505(b)(1) Fair Opportunity*.

The Government intends to issue a single award task order (hereinafter “prospective Task Order”) as a result of this Fair Opportunity Notice of Intent (hereinafter “Solicitation”) and incorporate the content of Sections B through E of this Solicitation into the prospective Task Order award. Sections F through H are provisional and will not be incorporated into the prospective Task Order unless otherwise stated in this Solicitation. The terms and conditions of the CIO-SP3 Small Business contract, in addition to or supplemented by the terms and conditions of this Solicitation, are applicable to the prospective Task Order. The prospective Task Order resulting from this Solicitation for commercial services will be awarded on Standard Form 1449.

Section B—Line Item Structure

Schedule of Services ¹				
CLIN	Description	Contract Type	Period of Performance ²	Price
Base Period				
0001	Product & Domain Level Testing	Labor Hour	06/01/2021 – 01/31/2022	
0002	RPA and AI/ML Engineering	Labor Hour	06/01/2021 – 01/31/2022	
0003	DevSecOps Teams	Labor Hour	06/01/2021 – 01/31/2022	
0004	Technical Governance Teams	Labor Hour	06/01/2021 – 01/31/2022	
0005	Program Management	Fixed Price	06/01/2021 – 01/31/2022	
0006	Verification System Testing – Optional	Labor Hour	06/01/2021 – 01/31/2022	
0007	NCAF ³	Lot	06/01/2021 – 01/31/2022	
Option Period 1				
1001	Product & Domain Level Testing	Labor Hour	02/01/2022 – 01/31/2023	
1002	RPA and AI/ML Engineering	Labor Hour	02/01/2022 – 01/31/2023	
1003	DevSecOps Teams	Labor Hour	02/01/2022 – 01/31/2023	
1004	Technical Governance Teams	Labor Hour	02/01/2022 – 01/31/2023	
1005	Program Management	Fixed Price	02/01/2022 – 01/31/2023	
1006	Verification System Testing – Optional	Labor Hour	02/01/2022 – 01/31/2023	
1007	NCAF	Lot	02/01/2022 – 01/31/2023	
Option Period 2				
2001	Product & Domain Level Testing	Labor Hour	02/01/2023 – 01/31/2024	
2002	RPA and AI/ML Engineering	Labor Hour	02/01/2023 – 01/31/2024	
2003	DevSecOps Teams	Labor Hour	02/01/2023 – 01/31/2024	

¹ Completed at time of award from the final agreed-to prices of Attachment H2. Attachment H2 will be included in the task order resulting from this solicitation.

² Completed at time of award. Offerors should assume a start date of June 1, 2021 for pricing purposes. See Section G for additional details.

³ NITAAC Contract Access Fee

2004	Technical Governance Teams	Labor Hour	02/01/2023 – 01/31/2024	
2005	Program Management	Fixed Price	02/01/2023 – 01/31/2024	
2006	Verification System Testing – Optional	Labor Hour	02/01/2023 – 01/31/2024	
2007	NCAF	Lot	02/01/2023 – 01/31/2024	
Option Period 3				
3001	Product & Domain Level Testing	Labor Hour	02/01/2024 – 01/31/2025	
3002	RPA and AI/ML Engineering	Labor Hour	02/01/2024 – 01/31/2025	
3003	DevSecOps Teams	Labor Hour	02/01/2024 – 01/31/2025	
3004	Technical Governance Teams	Labor Hour	02/01/2024 – 01/31/2025	
3005	Program Management	Fixed Price	02/01/2024 – 01/31/2025	
3006	Verification System Testing – Optional	Labor Hour	02/01/2024 – 01/31/2025	
3007	NCAF	Lot	02/01/2024 – 01/31/2025	
Option Period 4				
4001	Product & Domain Level Testing	Labor Hour	02/01/2025-01/31/2026	
4002	RPA and AI/ML Engineering	Labor Hour	02/01/2025-01/31/2026	
4003	DevSecOps Teams	Labor Hour	02/01/2025-01/31/2026	
4004	Technical Governance Teams	Labor Hour	02/01/2025-01/31/2026	
4005	Program Management	Fixed Price	02/01/2025-01/31/2026	
4006	Verification System Testing – Optional	Labor Hour	02/01/2025-01/31/2026	
4007	NCAF	Lot	02/01/2025-01/31/2026	

Section C—Task Order Clauses

The commercial item terms and conditions of the NITAAC CIO-SP3 Small Business Contract (“NITAAC Contract”) apply to this acquisition with the same force and effect as if written in their entirety herein. Additionally, the clauses contained in *Article I.1* of the NITAAC Contract apply to services performed on a fixed-price basis under the Fixed-Price Contract Line Item Numbers of the Task Order and the clauses contained in *Article I.3* of the NITAAC Contract apply to the services performed on a time and materials/labor hour basis under the Time & Materials or Labor Hour Contract Line Item Numbers of the Task Order. *Article I.5* Additional Contract Clauses of the NITAAC Contract also apply to this Task Order for commercial services. The clauses that appear below are either required to be re-stated in task orders or are in addition to the clauses of the NITAAC contract.⁴

C1. Federal Acquisition Regulation (FAR) Clauses Incorporated by Reference

52.252-2 - Clauses Incorporated by Reference (Feb 1998)

Includes amendments through FAC 2021-04, effective January 19, 2021.

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

FAR: <http://www.acquisition.gov/>

(End of clause)

Clause #	Title	Date
52.212-4	Contract Terms and Conditions-Commercial Items (Fixed Price CLINs ⁵)	Oct 2018
52.212-4 Alt. 1	Contract Terms and Conditions – Commercial Items - Alternate 1 (Labor Hour CLIN) Fill-ins completed as follows: (a)(4): “10%” (e)(1)(iii)(D): “Completed at Time of Award” or “None” if not completed at time of award (i)(1)(ii)(D)(1): “None” (i)(1)(ii)(D)(2): “None”	Oct 2018 Jan 2017
52.212-5	Contract Terms and Conditions Required to Implement Statutes or Executive Orders-Commercial Items* See C1.1 for the FAR 52.212-5(b) clauses applicable to this Task Order and which are not included in the NITAAC Contract. See C1.2 for Deviations from the FAR Clauses included in this FAR Clause.	Jan 2021

⁴ If a contract clause of this solicitation or the resulting task order conflicts with a contract clause of the NITAAC contract, the task order contract clause shall control.

⁵ Contract Line Item Numbers (CLINs). See Section B for the CLINs.

Clause #	Title	Date
52.217-9	Option to Extend the Term of the Contract: (a) “10 days before the contract expires” in the first blank, “30 days” in the second blank; (c) “56 months”	Mar 2000
52.237-3	Continuity of Services	Jan 1991
52.239-1	Privacy or Security Safeguards	Aug 1996
52.244-2	Subcontracts: (d) Completed at Time of Award; (j) Completed at Time of Award	Oct 2010
52.245-1	Government Property	Jan 2017
52.245-9	Use and Charges	Apr 2012

C1.1 Completion of FAR 52.212-5(b)

52.204-15 Service Contract Reporting Requirements (Oct 2016)

52.222-3 Convict Labor (Jun 2003)

52.224-3 Privacy Training (Jan 2017)

52.239-1 Privacy or Security Safeguards (Aug 1996)

(End of clause)

C1.2 FAR Clause Deviations

52.252-6 Authorized Deviations in Clauses (Nov 2020)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any Homeland Security Acquisition Regulation (48 CFR 3003 clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of clause)

52.204-23 Prohibition of Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lan and Other Covered Entities (July 2018) (DEVIATION 20-05)

(a) Definitions. As used in this clause-

"Covered article" means any hardware, software, or service that-

- (1) Is developed or provided by a covered entity;
- (2) Includes any hardware, software, or service developed or provided in whole or in part by a covered entity; or

(3) Contains components using any hardware or software developed in whole or in part by a covered entity.

"Covered entity" means-

- (1) Kaspersky Lab;
- (2) Any successor entity to Kaspersky Lab;
- (3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or
- (4) Any entity of which Kaspersky Lab has a majority ownership.

(b) Prohibition. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any covered article. The contractor is prohibited from-

- (1) Providing any covered article that the Government will use on or after October 1, 2018; and
- (2) Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.

(c) Reporting requirement.

(1) In the event the contractor identifies covered article provided to the Government during contract performance, or the contractor is notified of such by a subcontractor at any tier or by any other source, the contractor shall report, in writing, via email, to the Contracting Officer, Contracting Officer's Representative, and the Enterprise Security Operations Center (SOC) at NDAA Incidents@hq.dhs.gov, with required information in the body of the email. In the case of the Department of Defense, the contractor shall report to the website at <https://dibnet.dod.mil>. For indefinite delivery contracts, the contractor shall report to the Enterprise SOC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at <https://dibnet.dod.mil>.

(2) The contractor shall report the following information pursuant to paragraph (c)(1) of this clause:

- (i) Within 1 business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.
- (ii) Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the contractor shall describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.

(d) Subcontracts. The contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts, including subcontracts for the acquisition of commercial items.

(End of clause)

52.212-5 Deviations (From the Incorporated Clause in Section C1, above)

Replace (3) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2020) (Section 889(a)(1)(A) of Pub. L. 115-232) in FAR 52.212-5 with:

52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2020) (DEVIATION 20-05) (Dec 2020)

(a) Definitions. As used in this clause- "Backhaul" means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

"Covered foreign country" means The People's Republic of China.

"Covered telecommunications equipment or services" means-

- (1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
- (2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
- (3) Telecommunications or video surveillance services provided by such entities or using such equipment; or,
- (4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

"Critical technology" means-

- (1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;
- (2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening.

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

"Interconnection arrangements" means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

"Reasonable inquiry" means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

"Roaming" means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

"Substantial or essential component" means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition. (1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4 .2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) Exceptions. This clause does not prohibit contractors from providing- (1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement. (1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause in writing via email to the Contracting Officer, Contracting Officer's Representative, and the Network Operations Security Center (NOSC) at NDAA Incidents@hg.dhs.gov, with required information in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at <https://dibnet.dod.mil>. For indefinite delivery contracts, the Contractor shall report to the NOSC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at <https://dibnet.dod.mil>.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause (i) Within one business day from the date of such identification or notification: the contract number; the order number (s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended. (ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any

additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

52.219-14 Limitations on Subcontracting (DEVIATION 19-01) (AUG 2020)

(a) This clause does not apply to the unrestricted portion of a partial set-aside.

(b) Definition. “Similarly situated entity,” as used in this clause, means a first-tier subcontractor, including an independent contractor, that—

- (1) Has the same small business program status as that which qualified the prime contractor for the award (e.g., for a small business set-aside contract, any small business concern, without regard to its socioeconomic status); and
- (2) Is considered small for the size standard under the North American Industry Classification System (NAICS) code the prime contractor assigned to the subcontract.

(c) Applicability. This clause applies only to—

- (1) Contracts that have been set aside for any of the small business concerns identified in 19.000(a)(3);
- (2) Part or parts of a multiple-award contract that have been set aside for any of the small business concerns identified in 19.000(a)(3);
- (3) Contracts that have been awarded on a sole-source basis in accordance with subparts 19.8, 19.13, 19.14, and 19.15;
- (4) Orders expected to exceed the simplified acquisition threshold and that are—
 - (i) Set aside for small business concerns under multiple-award contracts, as described in 8.405-5 and 16.505(b)(2)(i)(F); or
 - (ii) Issued directly to small business concerns under multiple-award contracts as described in 19.504(c)(1)(ii);
- (5) Orders, regardless of dollar value, that are—
 - (i) Set aside in accordance with subparts 19.8, 19.13, 19.14, or 19.15 under multiple-award contracts, as described in 8.405-5 and 16.505(b)(2)(i)(F); or
 - (ii) Issued directly to concerns that qualify for the programs described in subparts 19.8, 19.13, 19.14, or 19.15 under multiple-award contracts, as described in 19.504(c)(1)(ii); and,
- (6) Contracts using the HUBZone price evaluation preference to award to a HUBZone small business concern unless the concern waived the evaluation preference.

(d) Independent contractors. An independent contractor shall be considered a subcontractor.

(e) Limitations on subcontracting. By submission of an offer and execution of a contract, the contractor agrees that, in performance of a contract assigned a North American Industry Classification System (NAICS) code for—

- (1) Services (except construction), it will not pay more than 50 percent of the amount paid by the Government for contract performance to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count towards the prime contractor's 50 percent subcontract amount that cannot be exceeded. When a contract includes both services and supplies, the 50 percent limitation shall apply only to the service portion of the contract;
- (2) Supplies (other than procurement from a non- manufacturer of such supplies), it will not pay more than 50 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count towards the prime contractor's 50 percent subcontract amount that cannot be exceeded. When a contract includes both supplies and services, the 50 percent limitation shall apply only to the supply portion of the contract;
- (3) General construction, it will not pay more than 85 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count towards the of 23 prime contractor's 85 percent subcontract amount that cannot be exceeded; or,
- (4) Construction by special trade contractors, it will not pay more than 75 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count towards the prime contractor's 75 percent subcontract amount that cannot be exceeded.

(f) The contractor shall comply with the limitations on subcontracting as follows:

- (1) For contracts, in accordance with paragraphs (c)(1), (2), (3), and (6) of this clause – Contracting Officer check as appropriate.
 - ☐ By the end of the base term of the contract and then by the end of each subsequent option period; or,
 - ☒ By the end of the performance period for each order issued under the contract.
- (2) For orders, in accordance with paragraphs (c)(4) and (5) of this clause, by the end of the performance period for the order.

(g) A joint venture agrees that, in the performance of the contract, the applicable percentage specified in paragraph (e) of this clause will be performed by the aggregate of the joint venture participants.

(End of clause)

**52.232-40 Providing Accelerated Payments to Small Business Subcontractors (Dec 2013)
(DEVIATION APR 2020)**

- (a)(1) In accordance with 31 U.S.C. 3903 and 10 U.S.C. 2307, upon receipt of

accelerated payments from the Government, the contractor shall make accelerated payments to its small business subcontractors under this contract in accordance with the accelerated payment date established, to the maximum extent practicable and prior to when such payment is otherwise required under the applicable contract or subcontract, with a goal of 15 days after receipt of a proper invoice and all other required documentation from the small business subcontractor if a specific payment date is not established by contract.

(2) The contractor agrees to make such payments to its small business subcontractors without any further consideration from or fees charged to the subcontractor.

(b) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.

(c) Include the substance of this clause, including this paragraph (c), in all subcontracts with small business concerns, including subcontracts with small business concerns for the acquisition of commercial items.

(End of clause)

C2. Homeland Security Acquisition Regulation (HSAR) Clauses Incorporated by Reference

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

HSAR: <https://www.dhs.gov/publication/hsar>

Clause #	Title	Date
3052.203-70	Instructions for contractor Disclosure of Violations	Sep 2012
3052.205-70	Advertisements, Publicizing Awards, and Releases	Sep 2012
3052.242-72	Contracting Officers Representative	Dec 2003

(End of clause)

C3. Homeland Security Acquisition Regulation (HSAR) Clauses Incorporated in Full Text and other Regulatory Requirements

3052.204-71 Contractor Employee Access (Sep 2012) Alternate I (SEP 2012)

(a) Sensitive Information, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Pub. L. 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training

concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange and complete any nondisclosure agreement furnished by DHS.

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and

(2) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the Contracting Officer.

(End of clause)

3052.209-73 Limitation of Future Contracting (Jun 2006)

- (a) The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest. Accordingly, the attention of prospective offerors is invited to FAR Subpart 9.5 --Organizational Conflicts of Interest.
- (b) The nature of this conflict is performing software development activities across the USCIS enterprise include the design of any software products or applications.
- (c) The restrictions upon future contracting are as follows:
- (1) The contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, shall be ineligible to perform, as a prime or first-tier subcontractor, an existing or future USCIS contract that requires the contractor to perform software development activities, including the design of any software products or applications. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the contractor, sufficient to avoid unfair competitive advantage or potential bias.
 - (2) If the contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work that are to be incorporated into a solicitation, the contractor shall be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under a future USCIS contract. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the contractor, sufficient to avoid unfair competitive advantage or potential bias. USCIS shall not unilaterally require the contractor to prepare such specifications or statements of work under this contract.
 - (2) To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with those other companies.

(End of clause)

HSAR Class Deviation 15-01: Safeguarding of Sensitive Information (MAR 2015)

(a) Applicability. This clause applies to the contractor, its subcontractors, and contractor employees (hereafter referred to collectively as “contractor”). The contractor shall insert the substance of this clause in all subcontracts.

(b) Definitions. As used in this clause— “Personally Identifiable Information (PII)” means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother’s maiden name. The definition of PII is not anchored to any single

category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

“Sensitive Information” is defined in *HSAR clause 3052.204-71, contractor Employee Access*, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107- 296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and ,

(4) Any information that is designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security

information handling procedures. “Sensitive Information Incident” is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, contractor system, or sensitive information.

“Sensitive Personally Identifiable Information (SPII)” is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver’s license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual’s name or other unique identifier plus one or more of the following elements:

- (1) Truncated SSN (such as last 4 digits)
- (2) Date of birth (month, day, and year)
- (3) Citizenship or immigration status
- (4) Ethnic or religious affiliation
- (5) Sexual orientation
- (6) Criminal History
- (7) Medical Information
- (8) System authentication information such as mother’s maiden name, account passwords or personal identification numbers (PIN)

Other PII may be “sensitive” depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) Authorities. The contractor shall follow all current versions of Government policies and guidance accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>, or available upon request from the Contracting Officer, including but not limited to:

- (1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
- (2) DHS Sensitive Systems Policy Directive 4300A
- (3) DHS 4300A Sensitive Systems Handbook and Attachments
- (4) DHS Security Authorization Process Guide
- (5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
- (6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
- (7) DHS Information Security Performance Plan (current fiscal year)
- (8) DHS Privacy Incident Handling Guidance

(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at

<http://csrc.nist.gov/groups/STM/cmvp/standards.html>

(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at <http://csrc.nist.gov/publications/PubsSPs.html>

(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at <http://csrc.nist.gov/publications/PubsSPs.html>

(d) Handling of Sensitive Information. contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how Contractors must handle sensitive but unclassified information. DHS uses the term “FOR OFFICIAL USE ONLY” to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook provide the policies and procedures on security for Information Technology (IT) resources. The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provides guidelines to help safeguard SPII in both paper and electronic form. DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the contractor except as specified in the contract.

(3) All contractor employees with access to sensitive information shall execute DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA), as a condition of access to such information. The contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The contractor shall provide copies of the signed NDA to the Contracting Officer’s Representative (COR) no later than two (2) days after execution of the form.

(4) The contractor’s invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) Authority to Operate. The contractor shall not input, store, process, output, and/or transmit sensitive information within a contractor IT system without an Authority to

Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) *Complete the Security Authorization process.* The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A (Version 11.0, April 30, 2014)*, or any successor publication, *DHS 4300A Sensitive Systems Handbook (Version 9.1, July 24, 2012)*, or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) *Security Authorization Process Documentation.* SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) *Independent Assessment.* Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) *Support the completion of the Privacy Threshold Analysis (PTA)* as needed. As part of the SA process, the contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act

System of Records Notice (SORN), or modifications thereto, are required. The contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at <http://www.dhs.gov/privacy-compliance>.

(2) *Renewal of ATO*. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The contractor is required to update its SA package as part of the ATO renewal process. The contractor shall update its SA package by one of the following methods:

(1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or,

(2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90-day review process is independent of the system production date and therefore it is important that the contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the contractor environment to ensure controls are in place.

(3) *Security Review*. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring*. All contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the Fiscal Year 2014 DHS Information Security

Performance Plan, or successor publication. The plan is updated on an annual basis. The contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with FIPS 140-2 Security Requirements for Cryptographic Modules and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of contractor systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for contractor systems.

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with 4300A Sensitive Systems Handbook Incident Response and Reporting requirements. When notifying the Headquarters or Component SOC, the contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the contractor shall use FIPS 140-2 Security Requirements for Cryptographic Modules compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in 4300A Sensitive Systems Handbook Incident Response and Reporting, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

- (i) Data Universal Numbering System (DUNS);
- (ii) Contract numbers affected unless all contracts by the company are affected;
- (iii) Facility CAGE code if the location of the event is different than the prime contractor location;
- (iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
- (v) Contracting Officer POC (address, telephone, email);
- (vi) Contract clearance level;
- (vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
- (viii) Government programs, platforms or systems involved;
- (ix) Location(s) of incident;
- (x) Date and time the incident was discovered;
- (xi) Server names where sensitive information resided at the time of the incident, both at the contractor and subcontractor level;
- (xii) Description of the Government PII and/or SPII contained within the system;
- (xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
- (xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

- (i) Inspections;
- (ii) Investigations;
- (iii) Forensic reviews, and,

(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) *Additional PII and/or SPII Notification Requirements.*

(1) The contractor shall have in place procedures and the capability to notify any individual whose PII resided in the contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the DHS Privacy Incident Handling Guidance. The contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

- (i) A brief description of the incident;
- (ii) A description of the types of PII and SPII involved;
- (iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
- (iv) Steps individuals may take to protect themselves;
- (v) What the contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and,
- (vi) Information identifying who individuals may contact for additional information.

(i) **Credit Monitoring Requirements.** In the event that a sensitive information incident involves PII or SPII, the contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the contractor or resided in the contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the contractor has no affiliation. At a minimum, credit monitoring services shall include:

- (i) Triple credit bureau monitoring;
- (ii) Daily customer service;
- (iii) Alerts provided to the individual for changes and fraud; and,
- (iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

- (i) A dedicated telephone number to contact customer service within a fixed period;
- (ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
- (iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics; (MAR 2015)
- (iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
- (v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
- (vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the contractor shall submit the certification to the COR and the Contracting Officer following the template provided in NIST Special Publication 800-88 Guidelines for Media Sanitization.

(End of clause)

HSAR Class Deviation 15-01: Information, Technology, Security and Privacy Training (Mar 2015)

(a) *Applicability.* This clause applies to the contractor, its subcontractors, and contractor employees (hereafter referred to collectively as “contractor”). The contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements.*

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user’s responsibilities change. The Department of Homeland Security (DHS) requires that contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each

year. Any new contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. The contractor shall maintain copies of training certificates for all contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The contractor shall maintain signed copies of the DHS Rules of Behavior for all contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) *Privacy Training Requirements.* All contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. HSAR Class Deviation 15-01 Attachment 1: Safeguarding of Sensitive Information (MAR 2015) Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The contractor shall maintain copies of training certificates for all contractor and subcontractor employees as a record of compliance. Initial training certificates for each contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The email notification shall state the required training has been completed for all contractor and subcontractor employees.

(End of clause)

3052.215-70 Key Personnel or Facilities (Dec 2003)

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before replacing any of the specified individuals or facilities, the contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The contractor shall not replace personnel or facilities until the Contracting Officer approves the change.

(c) The Key Personnel under this Contract are *(completed at time of award, if applicable based on the PWS which may include Key Personnel in addition to the Key Personnel listed below)*:

- Program Manager
- Fill-In
- Fill-In

(End of clause)

D – Other Task Order Requirements**D1. Period of Performance**

See Section (B) for the anticipated Period of Performance. The initial or base Period of Performance may be extended in yearly increments in accordance with *FAR 52.217-9 Option to Extend the Term of the Contract (March 2000)*. The Section B Period of Performance dates will be adjusted at the time of award. Offerors should assume a Period of Performance start date of June 1, 2021 for pricing purposes.

D2. Place of Performance

No Government facilities are available for performing the task order. Space is available at USCIS Headquarters at 5900 Capital Gateway Dr in Camp Springs, MD on a reservation basis; however, the space is not guaranteed and the Contractor should not assume performance at any Government facility.

D3. Performance Reporting

The Government intends to record and maintain contractor performance information for this task order, in accordance with FAR Subpart 42.15, on the contractor Performance Assessment Reporting System (CPARS) at <http://www.cpars.gov>. Contractor's representative is allotted a

60-day review/comment period starting from the date the Assessing Official forwarded the evaluation. If the contractor Representative does not provide comments within the 60-day period, the evaluation is then returned to the Assessing Official and the contractor Representative will no longer have access to enter comments. The Government will have to complete the evaluation without the contractor Representative comments. Within the first seven days of the comment period, the contractor Representative may request a meeting with the Assessing Official to discuss the evaluation. The contractor is encouraged to enroll at www.cpars.gov so it can participate in this process. The failure of the contractor Representative to provide comments within the 60-day period shall represent the contractor's acceptance of the performance assessment.

D4. Government Furnished Property

The Government will furnish the property listed in Attachment E3 to the contractor upon or soon after the award date of the Task Order. The Government will not be obligated to provide additional accessories for the laptop computers, e.g., monitors, computer bags, external mice, etc. See FAR clauses *52.245-1 Government Property* and *52.245-9 Use and Charges*.

D5. Government Furnished Information

Attachment E4 includes information to assist the contractor with performing the Task Order. (Attachment E4 may also assist offerors with the preparation of the offer. See Section G for Instruction to Offerors regarding submitting an offer for award of the prospective Task Order).⁶

D6. Performance Work Statement

The contractor shall perform in accordance with the terms and conditions of the Performance Work Statement (PWS). (The PWS will be incorporated into the prospective Task Order at the time of award. See Section G for additional information and instructions for submitting an offer, including a PWS.

D7. Training

The contractor is required to provide any all training necessary for the performance of the Task Order. The price for performing the Task Order includes any training cost, i.e., the Government will not reimburse the contractor for the cost of any training that may be required.

D8.

Reserved.

⁶ This parenthetical sentence will be deleted from the prospective task order at the time of award.

D9.

Reserved.

D10. Additional Invoicing Instructions

(a) USCIS' preferred method for invoice submission is electronically. Invoices shall be submitted in Adobe pdf format with each pdf file containing only one invoice. The pdf files shall be submitted electronically to USCISInvoice.Consolidation@ice.dhs.gov with each email conforming to a size limit of 500 KB.

(b) If a paper invoice is submitted, mail the invoice to:

**USCIS Invoice Consolidation
PO Box 1000
Williston, VT 05495
(802) 288-7600**

(c) All written approvals for travel shall be included with the submitted invoice.

(d) The contractor shall provide the details of the elements billed for itself as the "prime contractor" and for each subcontractor. The details shall be by period of performance per each CLIN, by labor classification, by number of labor hours, by labor rate, other direct costs (ODC) line items; and any applied indirect rates and base rates so the Government can verify billed amounts in the invoice. The contractor shall include source documents to support billed ODCs for the Government to verify allowability in accordance with FAR Part 31. The calculation of labor hours, labor rate, labor price any application of indirect costs to ODCs and total price billed shall be submitted in an Excel file, unlocked and include formulas, i.e., be accessible. These details shall be provided via email to the Contracting Officer and the COR. In addition, each invoice shall include a table and illustrative graph for each exercised Labor Hour CLIN showing the projected hours for each labor category across the entire period of performance and the actual hours incurred for every invoicing period to date. See also FAR 52.212-4(i) Alt. 1 for additional details that may be required to substantiate invoices for work performed on a labor-hour basis.⁷

(e) Direct Payment Inquiries to ICE Financial Operations at (877) 491.6521.

D11. Security and Privacy Controls

HSAR Class Deviation 15-01 – Safeguarding of Sensitive Information (c)(10) requires contractors to follow all current versions of the "National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at <https://csrc.nist.gov/publications/sp>. With USCIS retaining responsibility for all electronic technology security (e.g., servers, desktops, networking, communications, applications, software, databases, etc.), the contractor will be responsible for a

⁷ See also FAR 52.212-4(i) Alt. 1 for additional details that may be required to substantiate invoices for work performed on a labor-hour basis (the Labor Hour type CLINs).

limited set of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security and privacy controls for physical security:

- Access Control (AC) – AC-2
- Awareness and Training (AT) – AT-1, AT-2, AT-3, and AT-4
- Incident Response (IR) – IR-1, IR-2, IR-3, IR-4, and IR-8
- Physical and Environmental Protection (PE) – PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-7, PE-8, PE-9, PE-10, PE-11, PE-12, PE-13, PE-14, and PE-15
- Contingency Planning (CP) – CP-1, CP-2, CP-3, and CP-4
- Security Assessment and Authorization (CA) – CA-1, CA-2, CA-3, CA-4, CA-5, and CA-6
- Security Planning Policy (PL) – PL-1, PL-2, and PL-4
- Personnel Security (PS) – PS-1, PS-2, PS-3, PS-4, and PS-5

D12.

Reserved.

D13. Security Requirements (Commonly referred to as “Security Requirement 5”)

See Attachment E2 titled “U.S. Citizenship and Immigration Services Office of Security and Integrity – Personnel Security Division” dated August 2020.

D.14 Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 29 U.S.C. § 794d)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Appendix A, C & D, and available at <https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf>. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards. ICT includes IT and other equipment.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018, or any successor publication.

1. When developing or modifying ICT, the contractor is required to validate ICT deliverables for conformance to the applicable Section 508 requirements. Validation shall occur on a frequency that ensures Section 508 requirements is evaluated within each iteration and release that contains user interface functionality.
2. When modifying, installing, configuring or integrating commercially available or government-owned ICT, the contractor shall not reduce the original ICT Item's level of Section 508 conformance.
3. When developing or modifying web based and electronic content components, except for electronic documents and non-fillable forms provided in a Microsoft Office or Adobe PDF format, the contractor shall demonstrate conformance to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria) by conducting testing using the DHS Trusted Tester for Web Methodology Version 5.0 or successor versions, and shall ensure testing is conducted by individuals who are certified by DHS on version 5.0 or successor versions (e.g. "DHS Certified Trusted Testers"). The contractor shall provide the Trusted Tester Certification IDs to DHS upon request. Information on the DHS Trusted Tester for Web Methodology Version 5.0, related test tools, test reporting, training, and tester certification requirements is published at <https://www.dhs.gov/trusted-tester>.
4. When developing or modifying ICT deliverables that contain the ability to automatically generate electronic documents and forms in Microsoft Office and Adobe formats, or when the capability is provided to enable end users to design and author web based electronic content (i.e. surveys, dashboards, charts, data visualizations, etc.), the contractor shall demonstrate the ability to ensure these outputs conform to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria). The contractor shall demonstrate conformance by conducting testing and reporting test results based on representative sample outputs. For outputs produced as Microsoft Office and Adobe PDF file formats, the contractor shall use the test methods published under "Accessibility Tests for Documents", which are published at <https://www.dhs.gov/compliance-test-processes>. For outputs produced as web based electronic content, the contractor shall use the DHS Trusted Tester for Web Methodology Version 5.0, or successor versions. This methodology is published at <https://www.dhs.gov/trusted-tester>

Section 508 Deliverables

1. **Section 508 Test Plans:** When developing or modifying ICT pursuant to this contract, the contractor shall provide a detailed Section 508 Conformance Test Plan. The Test Plan shall describe the scope of components that will be tested, an explanation of the test process that will be used, when testing will be conducted during the project development life cycle, who will conduct the testing, how test results will be reported, and any key assumptions.

2. **Section 508 Test Results:** When developing or modifying ICT pursuant to this contract, the contractor shall provide test results in accordance with the Section 508 Requirements for Technology Services provided in this solicitation.
3. **Section 508 Accessibility Conformance Reports:** For each ICT item offered through this contract (including commercially available products, and solutions consisting of ICT that are developed or modified pursuant to this contract), the Offeror shall provide an Accessibility Conformance Report (ACR) to document conformance claims against the applicable Section 508 standards. The ACR shall be based on the Voluntary Product Accessibility Template Version 2.0 508 (or successor versions). The template can be found at <https://www.itic.org/policy/accessibility/vpat>. Each ACR shall be completed by following all of the instructions provided in the template, including an explanation of the validation method used as a basis for the conformance claims in the report.

D.15 Department of Homeland Security Enterprise Architecture Compliance

All solutions and services shall meet DHS and USCIS Enterprise Architecture and governance policies, standards, and procedures. Specifically, the contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) and USCIS governance requirements:

All developed solutions and requirements shall be compliant with the HLS and USCIS EA and governance processes.

All IT hardware and/or software shall be compliant with the DHS and USCIS EA Technical Reference Model (TRM) Standards and Products Profile.

Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS and USCIS Data Reference Model.

Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.

Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement.

All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

Section E—Task Order Schedule of Attachments

Number	Title of Document	# of Pages	Date	Comment
E1	Statement of Objectives	10	November 2020	
E2	Security Requirement 5	5	August 2020	
E3	Government Furnished Property	1	January 2021	
E4	Government Furnished Information	6	May 2020	The information may also assist offerors with preparing an offer to perform the prospective Task Order. ⁸
E5	Performance Work Statement (PWS)	Completed at time of award.	Completed at time of award.	The PWS offered by the successful offeror (contractor) shall be attachment to the prospective Task Order at the time of award. ⁹

Section F—Notice Provisions

F1. FAR & HSAR Solicitation Provisions

F1.1. FAR and HSAR Solicitation Provisions Incorporated by Reference

52.252-1 Solicitation Provisions Incorporated by Reference (Feb 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es):

www.acquisition.gov

<https://www.dhs.gov/publication/hsar>

Provision #	Title	Date
52.204-7	System for Award Management	Oct 2018
52.212-3	Offeror Representations and Certifications-Commercial Items	Jan 2021

(End of provision)

⁸ Comment will be deleted from the prospective task order at the time of award.

⁹ Comment will be deleted from the prospective task order at the time of award.

F1.2. Full Text of FAR & HSAR Solicitation Provisions**52.252-5 Authorized Deviations in Provisions (Nov 2020)**

(a) The use in this solicitation of any Federal Acquisition Regulation (48 CFR Chapter 1) provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the provision.

(b) The use in this solicitation of any Homeland Security Acquisition Regulation (48 Chapter 30) provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of provision)

52.204-8 Annual Representations and Certifications (Mar 2020) (DEVIATION 20-07) (July 2020)

(a)(1) The North American Industry Classification System (NAICS) code for this acquisition is 541512.

(2) The small business size standard is \$30M.

(3) The small business size standard for a concern which submits an offer in its own name, other than on a construction or service contract, but which proposes to furnish a product which it did not itself manufacture, is 500 employees.

(b)(1) If the provision at 52.204-7, System for Award Management, is included in this solicitation, paragraph (d) of this provision applies.

(2) If the provision at 52.204-7, System for Award Management, is not included in this solicitation, and the Offeror has an active registration in the System for Award Management (SAM), the Offeror may choose to use paragraph (d) of this provision instead of completing the corresponding individual representations and certifications in the solicitation. The Offeror shall indicate which option applies by checking one of the following boxes:

☐ (i) Paragraph (d) applies.

☐ (ii) Paragraph (d) does not apply and the offeror has completed the individual representations and certifications in the solicitation.

(c)(1) The following representations or certifications in SAM are applicable to this solicitation as indicated:

(i) 52.203-2, Certificate of Independent Price Determination. This provision applies to solicitations when a firm-fixed-price contract or fixed-price contract with economic price adjustment is contemplated, unless—

(A) The acquisition is to be made under the simplified acquisition procedures in Part 13;

(B) The solicitation is a request for technical proposals under two-step sealed bidding procedures; or

(C) The solicitation is for utility services for which rates are set by law or regulation.

(ii) 52.203-11, Certification and Disclosure Regarding Payments to Influence Certain

Federal Transactions. This provision applies to solicitations expected to exceed \$150,000.

(iii) 52.203-18, Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements—Representation. This provision applies to all solicitations.

(iv) 52.204-3, Taxpayer Identification. This provision applies to solicitations that do not include provision at 52.204-7, System for Award Management.

(v) 52.204-5, Women-Owned Business (Other Than Small Business). This provision applies to solicitations that—

(A) Are not set aside for small business concerns;

(B) Exceed the simplified acquisition threshold; and

(C) Are for contracts that will be performed in the United States or its outlying areas.

(vi) 52.204-26, Covered Telecommunications Equipment or Services—Representation. This provision applies to all solicitations.

(vii) 52.209-2, Prohibition on Contracting with Inverted Domestic Corporations—Representation.

(viii) 52.209-5, Certification Regarding Responsibility Matters. This provision applies to solicitations where the contract value is expected to exceed the simplified acquisition threshold.

(ix) 52.209-11, Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law. This provision applies to all solicitations.

(x) 52.214-14, Place of Performance—Sealed Bidding. This provision applies to invitations

for bids except those in which the place of performance is specified by the Government.

(xi) 52.215-6, Place of Performance. This provision applies to solicitations unless the place of performance is specified by the Government.

(xii) 52.219-1, Small Business Program Representations (Basic, Alternates I, and II). This provision applies to solicitations when the contract will be performed in the United States or its outlying areas.

(A) The basic provision applies when the solicitations are issued by other than DoD, NASA, and the Coast Guard.

(B) The provision with its Alternate I applies to solicitations issued by DoD, NASA, or the Coast Guard.

(C) The provision with its Alternate II applies to solicitations that will result in a multiple award contract with more than one NAICS code assigned.

(xiii) 52.219-2, Equal Low Bids. This provision applies to solicitations when contracting by sealed bidding and the contract will be performed in the United States or its outlying areas.

(xiv) 52.222-22, Previous Contracts and Compliance Reports. This provision applies to solicitations that include the clause at 52.222-26, Equal Opportunity.

(xv) 52.222-25, Affirmative Action Compliance. This provision applies to solicitations, other than those for construction, when the solicitation includes the clause at 52.222-26, Equal Opportunity.

(xvi) 52.222-38, Compliance with Veterans' Employment Reporting Requirements. This provision applies to solicitations when it is anticipated the contract award will exceed the

simplified acquisition threshold and the contract is not for acquisition of commercial items.

(xvii) 52.223-1, Biobased Product Certification. This provision applies to solicitations that require the delivery or specify the use of USDA-designated items; or include the clause at 52.223-2, Affirmative Procurement of Biobased Products Under Service and Construction Contracts.

(xviii) 52.223-4, Recovered Material Certification. This provision applies to solicitations that are for, or specify the use of, EPA-designated items.

(xix) 52.223-22, Public Disclosure of Greenhouse Gas Emissions and Reduction Goals—Representation. This provision applies to solicitations that include the clause at 52.204-7.)

(xx) 52.225-2, Buy American Certificate. This provision applies to solicitations containing the clause at 52.225-1.

(xxi) 52.225-4, Buy American—Free Trade Agreements—Israeli Trade Act Certificate. (Basic, Alternates II and III.) This provision applies to solicitations containing the clause at 52.225-3.

(A) If the acquisition value is less than \$50,000, the basic provision applies.

(B) If the acquisition value is \$50,000 or more but is less than \$83,099, the provision with its Alternate II applies.

(C) If the acquisition value is \$83,099 or more but is less than \$100,000, the provision with its Alternate III applies.

(xxii) 52.225-6, Trade Agreements Certificate. This provision applies to solicitations containing the clause at 52.225-5.

(xxiii) 52.225-20, Prohibition on Conducting Restricted Business Operations in Sudan—Certification. This provision applies to all solicitations.

(xxiv) 52.225-25, Prohibition on Contracting with Entities Engaging in Certain Activities or Transactions Relating to Iran—Representation and Certifications. This provision applies to all solicitations.

(xxv) 52.226-2, Historically Black College or University and Minority Institution Representation. This provision applies to solicitations for research, studies, supplies, or services

of the type normally acquired from higher educational institutions.

(2) The following representations or certifications are applicable as indicated by the Contracting Officer:

___ (i) 52.204-17, Ownership or Control of Offeror.

___ (ii) 52.204-20, Predecessor of Offeror.

___ (iii) 52.222-18, Certification Regarding Knowledge of Child Labor for Listed End Products.

___ (iv) 52.222-48, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Certification.

___ (v) 52.222-52, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Certification.

___ (vi) 52.223-9, with its Alternate I, Estimate of Percentage of Recovered Material Content

for EPA-Designated Products (Alternate I only).

___ (vii) 52.227-6, Royalty Information.

___ (A) Basic.

___ (B) Alternate I.

___ (viii) 52.227-15, Representation of Limited Rights Data and Restricted Computer Software.

(d) The Offeror has completed the annual representations and certifications electronically in SAM accessed through <https://www.sam.gov>. After reviewing the SAM information, the Offeror verifies by submission of the offer that the representations and certifications currently posted electronically that apply to this solicitation as indicated in paragraph (c) of this provision have been entered or updated within the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), as of the date of this offer and are incorporated in this offer by reference (see FAR 4.1201); except for the changes identified below [offeror to insert changes, identifying change by clause number, title, date]. These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer.

(End of provision)

52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2020)

The Offeror shall not complete the representation at paragraph (d)(1) of this provision if the Offeror has represented that it “does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument” in the provision at 52.204–26, Covered Telecommunications Equipment or Services—Representation, or in paragraph (v) of the provision at 52.212–3, Offeror Representations and Certifications– Commercial Items.

(a) Definitions. As used in this provision –

Backhaul, covered telecommunications equipment or services, critical technology, interconnection arrangements, reasonable inquiry, roaming, and substantial or essential component have the meanings provided in the clause 52.204–25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) *Prohibition.* (1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract or extending or renewing a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) ([https:// www.sam.gov](https://www.sam.gov)) for entities excluded from receiving federal awards for “covered telecommunications equipment or services.”

(d) *Representations.* The Offeror represents that—

(1) It ☐ will, ☐ will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation. The Offeror shall provide the additional disclosure information required at paragraph (e)(1) of this section if the Offeror responds “will” in paragraph (d)(1) of this section; and

(2) After conducting a reasonable inquiry, for purposes of this representation, the Offeror represents that—

It ☐ does, ☐ does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The Offeror shall provide the additional disclosure information required at paragraph (e)(2) of this section if the Offeror responds “does” in paragraph (d)(2) of this section.

(e) *Disclosures.* (1) Disclosure for the representation in paragraph (d)(1) of this provision. If the Offeror has responded “will” in the representation in paragraph (d)(1) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(2) Disclosure for the representation in paragraph (d)(2) of this provision. If the Offeror has responded “does” in the representation in paragraph (d)(2) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(End of provision)

52.204-26 Covered Telecommunications Equipment or Services-Representation (Dec 2019)

(a) Definitions. As used in this provision, “covered telecommunications equipment or services” has the meaning provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) Procedures. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (<https://www.sam.gov>) for entities excluded from receiving federal awards for “covered telecommunications equipment or services”.

(c) Representation. The Offeror represents that it ☐ does, ☐ does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(End of provision)

52.216-1 Type of Contract (Apr. 1984)

The Government contemplates award of a hybrid type contract (firm-fixed price and labor hour type contract line items – See Section B, resulting from this solicitation.

(End of provision)

52.233-2 Service of Protest (Sep. 2006)

(a) Protests, as defined in section [33.101](#) of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the Contracting Officer (addressed as follows) by obtaining written and dated acknowledgment of receipt from anthony.w.pellegrino@uscis.dhs.gov (802) 872-4637.

(b) The copy of any protest shall be received in the office designated above within one day of filing a protest with the GAO.

(End of provision)

HSAR 3052.209-72 Organizational Conflict of Interest (Jun 2006)

(a) Determination. The Government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting is “software development activities across the USCIS enterprise, including software design activities.”

(b) If any such conflict of interest is found to exist, the Contracting Officer may (1) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the offeror and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded. After discussion with the offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the offeror may be found ineligible for award.

(c) Disclosure: The offeror hereby represents, to the best of its knowledge that:

___ (1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract, or

___ (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included a mitigation plan in accordance with paragraph (d) of this provision.

(d) Mitigation. If an offeror with a potential or actual conflict of interest or unfair competitive advantage believes the conflict can be avoided, neutralized, or mitigated, the offeror shall submit a mitigation plan to the Government for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan.

(e) Other Relevant Information: In addition to the mitigation plan, the Contracting Officer may require further relevant information from the offeror. The Contracting Officer will use all information submitted by the offeror, and any other relevant information known to DHS, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

(f) Corporation Change. The successful offeror shall inform the Contracting Officer within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divestitures that may affect this provision. (g) Flow-down. The contractor shall insert the substance of this clause in each first tier subcontract that exceeds the simplified acquisition threshold.

(End of provision)

Section G – Instructions to Offerors

G1. Peripheral Information

G1.1. *DHS Procurement Innovation Lab*. This acquisition is being conducted under the auspices of the DHS Procurement Innovation Lab (PIL). The PIL is a virtual lab that experiments with innovative techniques for increasing efficiencies in the procurement process and institutionalizing best practices. There is nothing offerors need to do differently for this requirement as a result of this acquisition being conducted under the auspices of the PIL. The PIL project team may reach out to successful and unsuccessful Offerors to assess effectiveness of the procurement process and the innovative techniques applied. The anonymous feedback will be used to further refine DHS procurement practices. Additional information on the PIL may be found here <https://www.dhs.gov/pil>.

G1.2. *General Guidance*. This is an acquisition for the commercial services offered for sale by holders of a NITAAC CIO-SP3 Small Business contract. The Government is seeking offers to perform the prospective Task Order that will achieve the objectives outlined in the Statement of Objectives (SOO) on the commercial terms and conditions detailed in this solicitation. This acquisition follows the general ordering procedures of the NITAAC CIO-SP3 Small Business contract and the requirements of *FAR Part 16.505 – Ordering* permitting the Contracting Officer wide latitude to develop ordering procedures commensurate with the requirement and which reduce the burden on offerors. Accordingly, this solicitation includes Instructions to Offerors, tailored to the subject solicitation and requirement; *FAR 52.212-3 Representations and Certifications of Offerors*; *FAR 52.212-4 Contract Terms and Conditions - Commercial Items*, tailored to include the terms and conditions, in addition to those of the applicable CIO-SP3 contract, against which the prospective Task Order will be awarded, that will apply to prospective Task Order; and, *FAR 52.212-5 – Contract Terms and Conditions Required to Implement Statutes or Executive Orders – Commercial Items*.

G1.3. *General Rules of Engagement*. This acquisition is conducted under *FAR Subpart 16.5 Indefinite-Delivery Contracts*; therefore, the procedural requirements of *FAR Subpart 15.3 - Source Selection* do not apply. The Government reserves the right to make award on initial offers. If the Government decides to conduct exchanges and allow revisions of offers, the Government may elect to allow revisions from the most highly rated offers, or, for administrative convenience, allow revisions from a subset of the most highly rated offers or in the alternative, with all the technically acceptable offers. The Government may conduct multiple rounds of exchanges on one offer to resolve previously unresolved matters without reengaging offers from other offerors with whom there is no need for further exchanges. The Government may reject any or all offers if such action is in the public interest and waive informalities and minor irregularities in offers received.

G1.4. *General Offer Assessment Terms and Definitions*. Although this is a *FAR Subpart 16.5* acquisition, the evaluation of offers nevertheless results in an assessment of the relative strengths, deficiencies, weaknesses, and risk of an offer. The Government will

consider all available information to assess performance risk. To aid offerors in the preparation of offers, a “Strength” is an aspect of an offer that demonstrates a strong understanding of the requirements of the prospective contract; a “Significant Strength” is an aspect of an offer that demonstrates ability and performance beyond that required to successfully perform the prospective contract and which will benefit the Government significantly or measurably; a “Weakness” is a flaw in the offer that increases the risk of unsuccessful contract performance; a “Deficiency” is a material failure of the offer or a combination of weaknesses evincing an unacceptable risk of unsuccessful contract performance; and, a “Risk” is a risk of unsuccessful contract performance.

G1.5. Multi-phase Procurement. This acquisition includes multiple phases. To be considered for award of the prospective Task Order, an offeror must participate in Phase 1. Offerors may be eliminated from the competition meaning their respective offer will receive no further consideration for award of the prospective contract following an evaluation of the Phase 1 Offer. Offerors invited to participated in Phase 2 must submit the Phase 2 portion of the offer to be considered for award of the prospective Task Order.

G2. Instructions to Offerors

G2.1. NAICS and Business Size Standard. For this acquisition, the North American Industry Classification System (NAICS) code is 541512 and the small business size standard is \$30M.

G2.2. Submission of Phase 1 Offer. Submit the signed and dated Phase 1 Offer via NITAAC eGOS with a copy to anthony.w.pellegrino@uscis.dhs.gov, joan.giard@uscis.dhs.gov, and christina.baldwin@uscis not later than *4:00 p.m., February XX, 2021*.

G2.3. Format of Offer. Unless other specified in the several sections of the offer, use traditional, 8 ½ x 11 formatting with one (1) inch margins and Times New Roman font, not less than twelve (12) point. Charts or graphs (if used) may be in Arial font not less than ten (10) point. Include both a MS Word and PDF versions of all non-price portions of the offer and MS Excel for the price portion of the Offer. The MS Excel file (Attachment H2) must include all formulas used to calculate the prices offered and shall be unlocked.

G2.4. Content of Phase 1 Offer. To be considered for award of the prospective Task Order resulting from this solicitation, the offeror shall submit

G2.4.1. Cover Page. The Cover Page must include:

- (a) The solicitation number;
- (b) The time specified in the solicitation for receipt of offers;
- (c) The name, address, telephone number, DUNS and CAGE of the Offeror;
- (d) A statement specifying the extent of agreement with all terms, conditions, and provisions included in this solicitation and agreement to furnish all services at the price(s) offered;
- (e) Names, titles, telephone numbers and email addresses of person(s) authorized to negotiate on the Offeror’s behalf with the Government in connection with this FON; and,

(f) Name, title, and signature of person authorized to sign the Offer, accompanied by evidence of that agent's authority.

Limit the Cover Page to one (1) page.

G2.4.2. Contractor Accounting System Certification. Submit a copy of the most recent annual certification submitted to the NITAAC Customer Support Center pursuant to Article C.3, paragraph h of the Offeror's respective NITAAC CIO-SP3 Small Business contract.

G2.4.3. Response to Phase I Questions. Offerors shall submit a response to the questions on Attachment H1 by completing and submitting Attachment H1. Do not modify the formatting of Attachment H1, i.e., do not change the margin sizes, the font, or font style. Attachment H1 includes additional instructions regarding the formatting designed to ensure fairness among all offerors regarding the word count limit.

G2.4.4. Past Performance Information. The Offeror shall submit information regarding past or current contracts (including Federal, State, and local government and private) for efforts similar to the scope and magnitude of the requirements of the prospective Task Order. The Offeror may provide information on problems encountered on the identified contracts and the Offeror's corrective actions. The Offeror may provide information on predecessor companies, key personnel who have relevant experience, or subcontractors that will perform major or critical aspects of the requirements of this Solicitation if the Offeror deems the information relevant to this acquisition. The identified contracts shall include:

- (i) The client/customer;
- (ii) Contract Number and Project Title;
- (iii) Scope of work;
- (iv) Start and end dates;
- (v) Dollar value;
- (vi) Contract type;
- (vii) Services provided;
- (viii) Major deliverables produced;
- (ix) Performance measures/service levels applied;
- (x) Any awards that were received for superior performance;
- (xi) Quality assurance;
- (xii) Risk management methodologies used; and,
- (xiii) Lines of communication used.

Include a table showing the client/customer and the contact information for the person(s) who can verify the information provided. Contracts with past performance information reported to CPARs and transmitted to PPIPRs are preferred but not mandatory.

Limit the response to not more than ten (10) pages.

G2.5. *Notification of Phase 1 Results.* The Government will evaluate Phase 1 of the Offer and notify the Offeror, via email from the Contracting Officer, whether its Offer is among the most highly rated. See *Section G4 – Evaluation of Offers and Contract Award* for the *Phase 1 Offer* evaluation process.

G2.5.1. If the Offeror is notified that its *Phase 1 Offer* is among the most highly rated, the Offeror shall proceed to *Phase 2*. The notice will include the date by which to submit the *Phase 2 Offer*.

G2.5.2. If the Offeror is notified that its *Phase 1 Offer* is not among the most highly rated, the Offeror will be notified that its *Phase 1 Offer*, and the Offeror itself, will not be considered for award. The notice will include the general basis for excluding the *Phase 1 Offer* and the Offeror from further consideration for award of the prospective contract.

G2.5.3. The Government intends to select not more than three (3) Offerors to proceed to *Phase 2*.

G2.6. *Phase 2 Offer.* Offerors notified of proceeding to *Phase 2* shall submit the *Phase 2 Offer* in accordance with the instructions provided in the *Phase 1* notice.

G2.6.1. *Content of Phase 2 Offer.*

G2.6.1.1. *Performance Work Statement.* The Offeror shall submit a resource-loaded Performance Work Statement, consistent with *FAR 37.602 Performance Work Statement*, for meeting the objectives detailed in the Statement of Objectives (SOO) and for performing all requirements of the prospective contract. The PWS must include all work elements necessary to perform the prospective contract; for example, contract management and oversight, special requirements/constraints (e.g., security compliance), deliverables, quality control, and performance standards. Limit the PWS to fifty (50) pages.

G2.6.1.2. *Price Proposal.* The Offeror shall submit a Price Proposal, using the Pricing Template, Attachment H2, for performing the requirements of the prospective contract as described in the Performance Work Statement. The Pricing Template stipulates the contract type for each of the six (6) elements of the Statement of Objectives. Section B of the Task Order will be completed at the time of award using the prices proposed by the offerors and agreed-to at the time of award. The price proposed must also:

- (i) Identify the labor categories proposed and offered to perform the prospective Task Order using the Pricing Template, Attachment H2. Include the reference to the PWS element for all labor categories and hours estimated to be performed for each PWS element (CLINS). Ensure the labor categories and hours estimated for performance of each PWS element are consistent with the information provided in the Pricing Template;
- (ii) Describe the skills and experience for each labor category offered; and,
- (iii) Identify the fixed loaded hourly rates offered as awarded under the CIO-SP3 contract;

- (iv) Identify the discount, if any, offered to perform the prospective contract;
- (v) Identify any subcontracts proposed;
- (vi) Detail the Offeror's process to determine that any subcontract prices are fair and reasonable; and,
- (vii) A separate price (CLIN) for the NITAAC Contract Access Fee (NCAF) identified as a separate contract line item number (CLIN).

There is no page limit for the Price Proposal (Attachment H2); however, do not supplement the Non-Price portions of the offer, or provide any information other than that required by the Price Proposal (Attachment H2).

G2.7. Administrative Requirements of the Offer. The Offeror shall include separately with its Phase 2 Offer:

- (a) A completed copy of the representations and certifications at FAR 52.212-3 (see FAR 52.212-3(b) for those representations and certifications that the offeror shall complete electronically);
- (b) Acknowledgment of Solicitation Amendments;
- (c) A statement specifying the extent of agreement with all terms, conditions, and provisions included in the solicitation. Offers that fail to furnish required representations or information, or reject the terms and conditions of the solicitation may be excluded from consideration.
- (d) A statement that the offeror agrees to hold the prices in its offer firm for a period of not less than ninety (90) calendar days from the date specified for receipt of offers.

G2.8. Late submissions, modifications, revisions, and withdrawals of offers. (1) Offerors are responsible for submitting offers, and any modifications, revisions, or withdrawals, so as to reach the Government office designated in the solicitation by the time specified in this solicitation. Any offer, modification, revision, or withdrawal of an offer received at the Government office designated in the solicitation after the exact time specified for receipt of offers is "late" and will not be considered unless it is received before award is made, the Contracting Officer determines that accepting the late offer would not unduly delay the acquisition; and – if it was transmitted through an electronic commerce method authorized by the solicitation, it was received at the initial point of entry to the Government infrastructure not later than 5:00 p.m. one working day prior to the date specified for receipt of offers; or, there is acceptable evidence to establish that it was received at the Government installation designated for receipt of offers and was under the Government's control prior to the time set for receipt of offers; or, it was the only offer received. However, a late modification of an otherwise successful offer, that makes its terms more favorable to the Government, will be considered at any time it is received and may be accepted. Offers may be withdrawn by written notice received at any time before the exact time set for receipt of offers.

G2.9 Page Limitation Table

The number of pages (length) of the Offer is limited as follows:

Offer Content	Page limit
Cover Page	1
Phase 1 Offer – <i>Response to Phase 1 Questions</i>	See Attachment H1
Phase 1 Offer – <i>Past Performance Information</i>	10
Phase 2 Offer – <i>Performance Work Statement</i>	50
Phase 2 Offer – <i>Administrative Requirements of the Offer</i>	N/A
Section 3: Price Proposal	See Attachment H2

G3. Additional Information

G3.1. *Incumbent contractor and Magnitude of Services.* This is a new procurement and does not follow-on any incumbent work. To assist offerors with assessing the magnitude of services to be performed during contract performance and to develop a resource-loaded Performance Work Statement, the Government estimates that approximate \$9.5M to \$11.5M of services are required to meet all requirement in a calendar/contract year basis.

G3.2. Points of Contact

All inquiries regarding this solicitation shall be addressed to the contracting officer via the NITAAC eGOS with a copy to the contract specialists at joan.giard@uscis.dhs.gov and christina.baldwin@uscis.dhs.gov.

G3.3. Solicitation Questions

A draft of this solicitation was posted to eGOS on or about Monday, February 1, 2021. The draft solicitation requested potential sources to submit questions regarding the solicitation. Therefore, any additional questions submitted regarding this solicitation will be responded to at the discretion of the Government.

G4. Evaluation of Offers and Contract Award

G4.1. The assessment of an offer will consider its respective, relative merit based upon a qualitative assessment consistent with the evaluation scheme described in section G4.2. While adjectives may be used to describe the relative merits of an offer, the Government will look beyond any adjectival ratings that may be used during the assessment to determine the relative merit of offers and to select the offeror deemed to provide the best value for performing the prospective contract.

G4.2. *Evaluation Scheme.* Consistent with *FAR Subpart 16.505(b)(iv)*, the significant factors as described above and which the agency expects to consider in evaluating Offers are (1)

Specialized Experience & Technical Competency; (2) *Past Performance*; (3) *Performance Work Statement*; and (4) *Price*. *Specialized Experience & Technical Competency* are the most important factors, followed by *Past Performance*, the *Performance Work Statement*, and *Price*. The evaluation factors are listed in the relative order of importance. When the evaluation factors are combined, *Specialized Experience & Technical Competence*, *Past Performance*, and the *Performance Work Statement* are more important than the *Price*.

G4.2.1. *Evaluation of the Phase 1 Offer – Specialized Experience and Technical Competence*. The Government will evaluate an offeror's Specialized Experience & Technical Competence using the offeror's response to the five (5) questions on Attachment H1 to assess the (1) the offeror's understanding of the Government's Objectives and the Outcomes to be achieved under the prospective Task Order as detailed in the SOO; and (2) the likelihood of the offeror successfully performing the prospective Task Order.

G4.2.2. *Evaluation of the Phase 1 Offer – Past Performance*. The Government will evaluate the Past Performance Information to assess the likelihood of the offeror successfully performing the prospective Task Order based on the quality of recent, relevant performance on contracts that are similar to that of the prospective Task Order. In the case of an offeror without a record of relevant past performance or for whom information on past performance is not available, the offeror may not be evaluated favorably or unfavorably on past performance.

G4.2.3. *Evaluation of the Phase 1 Offer - Exchange of Information*. An offeror may be invited to discuss aspects of its Phase 1 Offer to assist the Government with its evaluation of the Phase 1 Offer. This exchange of information will not result in a request for any revisions to the Phase 1 Offer. Rather, the exchange will provide an opportunity for the Offeror and the Government to discuss perceived ambiguities, and to provide greater clarity regarding the Offeror's response to the Phase 1 Offer.

G4.2.4. *Evaluation of the Phase 1 Offer - Notification*. Following the evaluation of the Phase 1 Offer, the Government will notify the Offeror that either (1) its Phase 1 Offer is not among the most highly rated and that it will not be proceeding to Phase 2 of the Offer; or, (2) that its Phase 1 Offer is among the most highly rated and that it will be proceeding to Phase 2. An offeror notified that its offer is not among the most highly rated will receive general information regarding its offer and the basis for the Government's decision. An offeror notified that its offer is among the most highly rated, will receive general comments regarding the Government's decision and will be notified of the date and time to submit the *Phase 2 Offer*.

G4.3. *Evaluation of the Phase 2 Offer – Performance Work Statement*. The Performance Work Statement will be evaluated to assess:

- (a) the Offeror's relative understanding of the Objectives and Outcomes detailed in the SOO;
- (b) the quality of the proposed services; and;

(c) the likelihood of the Performance Work Statement achieving the Objectives and Results of the SOO, i.e. successful performance of the prospective contract

G4.4. Evaluation of the Phase 2 Offer - Price Analysis. The Government will analyze the Price to ensure the final agreed-to price is fair and reasonable. The Government will use the analytical techniques of *FAR 15.404-1* to evaluate the reasonableness of the offered prices. The analytical techniques and procedures of *FAR 15.404-1* may be used, singly or in combination with others, to ensure that the final price is fair and reasonable. Certified cost or pricing data are not expected to be required and the Government expects to analyze and evaluate the Price using the first two (2) techniques of *FAR 15.404-1(b)(2)*. However, if the contracting officer determines that information on competitive proposed prices or previous contract prices is not available or is insufficient to determine that the price is fair and reasonable, the contracting officer may use any of the remaining techniques as appropriate to the circumstances applicable to the acquisition. This evaluation and analysis may include evaluating and analyzing the labor categories, number of hours per labor category, and labor category hourly rates to determine the need for, and reasonableness of, the proposed resources (sometimes referred to as the “labor mix”), assuming reasonable economy and efficiency. In accordance with *FAR 15.404-1(g)*, the Government may also determine that an offer is unacceptable if the prices proposed are materially unbalanced among the labor rates proposed, line items, or subline items. Unbalanced pricing exists when, despite an acceptable total evaluated price, the price of one or more labor categories, line items, or subline items is significantly overstated or understated as indicated by the application of price analysis techniques. An offer may be rejected if the Government determines that the lack of balance poses an unacceptable risk to the Government. Overall, the Government may use any of the techniques and processes in *FAR 15.401-1* to ensure the final agreed-to price is fair and reasonable and does not pose an unacceptable risk to the Government.

G4.5 Phase 2 Evaluation - Exchanges with Best-Suited Offeror. Once the Government determines the offeror that is the best-suited offeror (i.e., the apparent successful contractor), the Government reserves the right to communicate with only that offeror to address any remaining issues, if necessary, and finalize the prospective Task Order with that offeror. These issues may include technical and price. If the parties cannot successfully address any remaining issues, as determined pertinent at the sole discretion of the Government, the Government reserves the right to communicate with the next best-suited offeror based on the original analysis and address any remaining issues. Once the Government has begun communications with the next best-suited offeror, Government intends no further communications with the original best-suited offeror; however, the Government reserves the right to re-engage the prior best-suited offeror. This process shall continue until an agreement is successfully reached and the prospective Task Order is awarded.

G5. Award

A written award or acceptance of an Offer mailed or otherwise furnished to the successful Offeror within the time specified in the proposal shall result in a binding contract without further action by either party.

G6. Post-Award Administrative Matters

Debriefings. Notwithstanding that this Fair Opportunity Notice of Intent is being conducted pursuant to *FAR Subpart 16.505*, the contracting officer will, in accordance with *FAR 15.503(b)(1)*, notify Offerors who did not receive an award of the prospective contract. The procedures at *FAR 15.506* shall be followed when providing any post-award debriefings.

G7. Award Decision Documentation. The contracting officer will document the rationale for awarding, and the price of, the prospective Task Order including the basis for award and the rationale for any tradeoffs among the evaluation factors; however, the documentation need not quantify the tradeoffs that led to the decision.

SECTION H – PROVISIONAL ATTACHMENTS

Number	Name	Comment
H1	70SBUR20F00000027 – QISD Phase 1 Offer Questions	Complete and Return with Offer ¹⁰
H2	Price Proposal Template	Complete and Return with Offer. ¹¹
H3	Solicitation Question Template	For submitting Solicitation Questions

¹⁰ All or portions of the response to the Phase 1 Offer Questions may be incorporated into the prospective Task Order at the time of award.

¹¹ Final Agreed-to Price Proposal will be included in the prospective Task Order at the time of award.